**IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION**

| | | |
|---|---|---|
| SHANICE KLOSS, individually and on behalf of similarly situated individuals, | ) | |
| *Plaintiff*, | ) | No. 18-cv-7986 |
| v. | ) | Hon. John Robert Blakey |
| CASHCRATE, LLC, a Nevada limited liability company, and MH SUB I, LLC, D/B/A VBULLETIN, a Delaware limited liability company, | ) | Magistrate Judge Maria Valdez<br>**Jury Demanded** |
| *Defendants*. | ) | |

## FIRST AMENDED CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff, Shanice Kloss ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings her First Amended Class Action Complaint against Defendants CashCrate, LLC ("Defendant" or "CashCrate") and MH SUB I, LLC, d/b/a vBulletin ("vBulletin") (collectively, "Defendants"). Plaintiff alleges as follows based on personal knowledge as to her own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by her attorneys.

## INTRODUCTION

1. Defendant vBulletin is the global leading provider for forum software solutions for various private and public entities. Defendant vBulletin's forum software ("Forum Software") is used by tens of thousands of entities in order to provide their respective customers with the ability to communicate and collaborate in an online forum setting.

2. Defendant vBulletin not only markets its Forum Software as technically secure, but also boasts that its Forum Software includes "world-renowned technical support."

3. However, around or before August 2016, Defendant vBulletin discovered a catastrophic, SQL-injection-based vulnerability ("Software Vulnerability") in its Forum Software.

4. An SQL-injection-based vulnerability, such as the subject Software Vulnerability, allows hackers and other unauthorized third parties to input, or "inject," a malicious string of software code into an otherwise benign software code in order to accomplish nefarious objectives, such as the extraction of personal and confidential information.

5. Because SQL-injection-vulnerabilities are among the most common and widely-exploited vulnerabilities, an entity that employs reasonable cyber-risk management practices that include a robust patch management and notification program and regular monitoring of SQL-based statements is positioned to detect and mitigate, if not thwart altogether, SQL-based vulnerabilities and attacks.

6. Defendant vBulletin failed to implement reasonable cyber-risk management practices, particularly regarding its patch management program and regular SQL monitoring. By failing to reasonably detect the Software Vulnerability, and, even after detecting the Software Vulnerability, failing to implement a reasonable patch management and notification program, Defendant vBulletin allowed hackers to exploit the Software Vulnerability and extract the sensitive and confidential personal information, which includes but is not limited to names, home and business addresses, email addresses, demographic information, payment information and/or passwords (collectively, "PII"), of tens of millions of individuals throughout the United States.

7. Defendant CashCrate is a paid-survey-site that rewards its customers in exchange for completing various online surveys. At all relevant times, Defendant CashCrate utilized Defendant vBulletin's Forum Software.

8. Around or before November 2016, Defendant CashCrate learned that it had been the target of an SQL-injection attack ("Data Breach"), resulting in unauthorized outside parties gaining access to CashCrate's customers' PII, including their names, home and business addresses, email addresses, demographic information, and passwords.

9. Defendant vBulletin's Software Vulnerability created the access point through which the hackers were able to accomplish the Data Breach.

10. After exploiting the Software Vulnerability, hackers were able to extract the PII for over six million (6,000,000) of Defendant CashCrate's customers.

11. On information and belief, Defendant vBulletin's Software Vulnerability resulted in similar data breach incidents for dozens of Defendant vBulletin's Forum Software licensees, including Defendant CashCrate, in turn resulting in the unauthorized exposure of tens of millions of individuals throughout the United States.

12. Defendant CashCrate failed to implement a reasonable cyber-risk management program, including implementing technical safeguards to de-identify the PII, such as encryption, putting in place a reasonable procedure for vetting third-party vendors, such as Defendant vBulletin, and, critically, evaluating both prospectively and on an ongoing basis any third-party software, such as the subject Forum Software.

13. Defendant CashCrate also failed to implement a reasonable patch management program, which would have enabled it to significantly mitigate the scope of, or avoid entirely, the Data Breach. Finally, Defendant CashCrate failed to notify, let alone in a reasonable and timely manner, Plaintiff and the other class members that their PII was compromised in the Data Breach.

14. Plaintiff and the putative class members have all been injured as a direct result of Defendants' respective actions, omissions, and failures.

## PARTIES

15. Defendant CashCrate, LLC, is a Nevada limited liability company that is transacting business in Cook County, Illinois and maintains its headquarters in Nevada. Defendant CashCrate transacts, and intentionally seeks to transact, business with Illinois residents throughout the state of Illinois, including in Cook County, Illinois.

16. Defendant MH Sub I, LLC, d/b/a vBulletin, is a Delaware limited liability company that is licensed and registered by the Illinois Secretary of State to transact business in Illinois, including in Cook County. Defendant vBulletin transacts, and intentionally seeks to transact, business with Illinois residents throughout the state of Illinois, including in Cook County, Illinois

17. Plaintiff Shanice Kloss is a resident and citizen of the State of Illinois.

## JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this matter pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) *et seq.*, because this case is a class action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are greater than 100 putative class members; at least one putative class member is a citizen of a state other than Defendants; and none of the exceptions under subsection 1332(d) apply.

19. This Court may assert personal jurisdiction over Defendants because they conduct substantial business within Illinois and intentionally market their products to Illinois residents.

20. Venue is proper in this District because Plaintiff resides in this District and a substantial part of the events giving rise to Plaintiff's claims occurred in this District.

## FACTS SPECIFIC TO PLAINTIFF

21. In order to participate on Defendant CashCrate's paid-survey online website, Plaintiff was required to create an account and provide her PII to Defendant CashCrate.

22. On its paid-survey website, Defendant CashCrate licensed and implemented Defendant vBulletin's Forum Software in order to allow Defendant CashCrate's customers, like Plaintiff, the ability to chat with one another while on the paid-survey website.

23. However, Defendant vBulletin's Forum Software contained a Software Vulnerability that allowed hackers to carry out successful SQL-injection attacks on the information technology systems of vBulletin Forum Software licensees, including Defendant CashCrate.

24. The Software Vulnerability allowed hackers to extract the PII of millions of vBulletin Forum Software licensees' customers, including Plaintiff.

25. Despite being aware of the Software Vulnerability no later than August 2016, Defendant vBulletin failed to implement a reasonable patch management and notification protocol to alert its Forum Software Licensees about the Software Vulnerability and provide a patch to cure, or at least mitigate, the impact of the Software Vulnerability. Likewise, Defendant vBulletin failed to reasonably and regularly monitor its SQL-based code used in the Forum Software in the time leading up to its eventual discovery of the Software Vulnerability.

26. Around or before November 2016, Defendant CashCrate learned that it had been the target of an SQL-injection attack. Defendant CashCrate was not able to prevent, detect, thwart, or reasonably mitigate the Data Breach, resulting in exposure of the PII of over six million (6,000,000) of its customers. Defendant vBulletin's Software Vulnerability allowed hackers to carry out the successful SQL-injection attack on Defendant CashCrate's information systems.

27. Defendant CashCrate failed to implement a reasonable cyber-risk management program that included vetting Defendant vBulletin and its Forum Software prior to implementing the Forum Software, as well as procedures for ongoing evaluation and patch management of the Forum Software.

28. Defendant CashCrate also failed to notify, let alone in a reasonable and timely manner, Plaintiff and the other class members that their PII was compromised in the Data Breach

29. The PII exposed as a result of Defendants' respective cybersecurity practices includes password information. Because Defendant CashCrate failed to implement reasonable technical safeguards, including adequate encryption technology, the PII, including password data, once obtained via the SQL-injection attack, was easily decrypted by the hackers.

30. Despite the severity of the Data Breach, Defendant CashCrate failed to conduct a reasonable breach notification protocol. Aside from a passive support page, CashCrate failed to take measures to alert Plaintiff that her PII had been compromised in the Data Breach.

31. It was not until September 2018 that Plaintiff learned of the Data Breach through her own investigation and efforts.

32. Without identifying any justification, and in violation of the law, Defendant CashCrate failed to promptly and adequately notify Plaintiff of the Data Breach.

33. Given the current prevalence of cybersecurity awareness, including specifically SQL-injection attacks, Defendant vBulletin knew of the risks inherent in providing SQL-based software without also implementing reasonable SQL monitoring and patch management policies.

34. Likewise, Defendant CashCrate knew of the risks in capturing, storing, and using the PII of its customers and the consequences of the exposure of such PII to unauthorized third parties, as well as the importance of promptly notifying affected parties following the Data Breach.

35. Had Plaintiff been informed of the Data Breach within a reasonable period of time as required by law and/or through a reasonable manner and medium, Plaintiff and the other members of the putative class would have been able to take actions to protect their identities, accounts, and other potential targets from further misuse.

36. Defendants' respective failures to comply with reasonable data security standards provided them benefits in the form of saving on the costs of compliance, but at the expense and severe detriment of Plaintiff, whose PII has been exposed in the Data Breach and placed at serious and ongoing risk of imminent misuse and identity theft.

37. Since recently becoming aware of the Data Breach, Plaintiff has taken time and effort to mitigate her risk of identity theft, including monitoring her credit and financial accounts.

38. Plaintiff has also been harmed by having her PII compromised and faces the imminent and impending threat of future additional harm from the increased threat of identity theft and fraud due to her PII being sold, misappropriated, or otherwise misused by unknown parties.

39. Indeed, Plaintiff has suffered substantial privacy and informational injuries and, at the very least, faces the certainty of highly-targeted and ongoing spam and phishing campaigns.

40. Plaintiff has also experienced mental anguish as a result of the Data Breach. She experiences anxiety and anguish when thinking about what would happen if her identity is stolen as a result of the Data Breach; when wondering how long and to how many parties her PII was exposed before the Data Breach was even discovered or cured; and when she thinks about the fact that Defendant CashCrate was aware of the Data Breach and actively decided to keep her and the other victims of the Data Breach ignorant of the fact that their PII had been compromised.

41. The Data Breach was caused and enabled by Defendants' knowing violations of their respective obligations to abide by adequate cybersecurity practices in protecting PII.

## CLASS ALLEGATIONS

42. Plaintiff brings Counts I through VII, as set forth below, on behalf of herself and a Class and Subclass (together, the "Class," unless otherwise noted) of similarly situated individuals. The Class and Subclass are defined as follows:

> **Class:** All persons whose PII was in the possession of Defendant vBulletin, or in the possession of licensees of its Forum Software, while the Software Vulnerability was present.
>
> **Illinois Subclass:** All Illinois residents whose Personal Information was in the possession of Defendant vBulletin, or in the possession of licensees of its Forum Software, while the Software Vulnerability was present.

43. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendants; and any immediate family member of such officer or director.

44. Upon information and belief, there are millions of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of Class members is currently unknown, it is believed to be over six million (6,000,000) and can easily be ascertained through Defendants' records.

45. Plaintiff's claims are typical of the claims of the Class members she seeks to represent because the factual and legal bases of Defendants' liability to Plaintiff and the other Class members are the same and because Defendants' conduct has resulted in similar injuries to Plaintiff and to the Class members. As alleged herein, Plaintiff and the other Class members have all suffered damages as a result of Defendants' failure to maintain reasonable security safeguards.

46. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to:

a. Whether Defendant CashCrate adequately safeguarded Plaintiff's and the Class members' PII;

b. Whether Plaintiff and the Class members were notified of the Data Breach within a reasonable period of time and through a reasonable method;

c. Whether Defendant vBulletin failed to implement a reasonable patch notification program;

d. Whether there was an unauthorized disclosure of the Class members' PII;

e. When Defendant vBulletin first learned of the Software Vulnerability;

f. When Defendant CashCrate first learned of the Data Breach;

g. Whether Defendant vBulletin's Forum Software contained a Software Vulnerability, and if so, the time period in which the Software Vulnerability existed;

h. Whether Defendant CashCrate's cybersecurity prevention, detection, and notification protocols were reasonable under industry standards; and

i. Whether Defendants' conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*.

47. Absent a class action, most Class members would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

48. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class she seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the other Class members and have the financial resources to do so. Neither Plaintiff nor her counsel has any interest adverse to those of the other members of the Class.

49. Defendants have acted and failed to act on grounds generally applicable to the Plaintiff and the other Class members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

## COUNT I
## Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq***.**
## (On behalf of Plaintiff and the Illinois Subclass Against Defendant CashCrate)

50. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

51. Pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*., Defendant CashCrate was required to implement and maintain reasonable security measures to protect the Plaintiff's and Illinois Subclass members' PII, and to notify them regarding any unauthorized disclosure in the most expedient time possible and without unreasonable delay.

52. Defendant CashCrate's unlawful conduct alleged herein in failing to safeguard its customers' PII, and subsequent failure to timely notify its customers that such PII had been compromised, constitute violations of the Illinois Personal Information Protection Act.

53. Pursuant to Section 530/20 of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*. ("ICFA"), a violation of the Illinois Personal Information Protection Act, as alleged herein, is itself deemed an "unlawful practice" and violation under the ICFA, and Defendant CashCrate has therefore violated the ICFA.

54. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant CashCrate's unlawful conduct and violations of the ICFA.

55. Wherefore, Plaintiff prays for relief as set forth below.

## COUNT II
## Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq***.**
## (On behalf of Plaintiff and the Illinois Subclass Against Defendant vBulletin)

56. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

57. Section 2 of the ICFA, 815 ILCS 505/2, prohibits entities such as Defendant vBulletin from engaging in unfair or deceptive business acts or practices.

58. Misrepresentations or the omission of a material fact constitute unfair, deceptive, or otherwise unlawful acts under the ICFA.

59. Defendant vBulletin's failures to implement reasonable SQL monitoring and patch management policies constitute unfair and/or deceptive business practices within the meaning of the ICFA when combined with Defendant vBulletin's explicit statements regarding the security and "world-renown" technical support it claims to offer its Forum Software licensees.

60. Plaintiff would not have utilized Defendant vBulletin's Forum Software, whether directly or through one of its licensees such as Defendant CashCrate, had she known of the Software Vulnerability or that Defendant vBulletin employs inadequate SQL monitoring and patch management practices.

61. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant vBulletin's unlawful conduct and violations of the ICFA.

62. Wherefore, Plaintiff prays for relief as set forth below.

## COUNT III
## Breach of Contract
## (On behalf of Plaintiff and the Class and Subclass Against Defendant CashCrate)

63. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

64. Plaintiff and the Class members are parties to express agreements with Defendant CashCrate whereby Plaintiff and the Class members provide their PII in exchange for paid-survey services and the provisioning of reasonable safeguards to prevent the unauthorized disclosure of their PII. Defendant CashCrate's business model depends on the extraction of data from customers, so it was incumbent on Defendant CashCrate to engage in reasonable cybersecurity practices.

65. Defendant CashCrate's failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of contract.

66. Plaintiff and the Class members would not have provided and entrusted their PII to Defendant CashCrate in the absence of an agreement to reasonably safeguard their PII and to reasonably notify them of unauthorized disclosures.

67. Plaintiff and the members of the Class fully performed their obligations under their contracts with Defendant CashCrate.

68. Defendant CashCrate breached the contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII and by failing to notify them in a timely and accurate manner that that their PII was compromised as a result of the Data Breach.

69. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant CashCrate's breaches of contract.

70. Wherefore, Plaintiff prays for the relief set forth below.

## COUNT IV
## Breach of Implied Contract
## (On behalf of Plaintiff and the Class and Subclass Against Defendant CashCrate)
## (in the alternative to Count III)

71. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

72. Plaintiff and the Class members were required to provide Defendant CashCrate their PII as a condition of using its paid-survey services. To the extent that it is found that an express contract did not exist, Defendant CashCrate entered into implied contracts with Plaintiff and the Class members whereby, by virtue of such requirement to provide their PII, Defendant CashCrate was obligated to take reasonable steps to secure and safeguard such PII and obligated to take reasonable steps following an unauthorized disclosure of the same.

73. Defendant CashCrate's failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of an implied contract.

74. Plaintiff and the members of the Class fully performed their obligations under their implied contracts with Defendant CashCrate.

75. Defendant CashCrate breached the implied contracts it made with Plaintiff and the Class members by failing to safeguard and protect their PII, and by failing to notify them in a timely and accurate manner that that their PII was compromised as a result of the Data Breach.

76. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant CashCrate's breaches of contract.

77. Wherefore, Plaintiff prays for the relief set forth below.

## COUNT V
### Breach of Implied Contract
### (On behalf of Plaintiff and the Class and Subclass Against Defendant vBulletin)

78. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

79. Plaintiff and the Class members entered into implied contracts with Defendant vBulletin whereby, by virtue of Plaintiff and the Class members utilizing Defendant vBulletin's Forum Software and providing their PII and Defendant vBulletin's representations regarding the security of the Forum Software, Defendant vBulletin was obligated to reasonably monitor its SQL-based Forum Software and take reasonable steps to secure and safeguard the PII following discovery of the Software Vulnerability, including by implementing a reasonable patch management protocol.

80. Defendant vBulletin's failure to implement adequate and reasonable SQL monitoring and patch management policies constitutes a breach of an implied contract.

81. Plaintiff and the members of the Class fully performed their obligations under their implied contracts with Defendant vBulletin.

82. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant vBulletin's breaches of contract.

83. Wherefore, Plaintiff prays for the relief set forth below.

## COUNT VI
## Negligence
## (On behalf of Plaintiff and the Class and Subclass Against Defendant CashCrate)

84. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

85. As a condition of using its paid-survey services, Defendant CashCrate required Plaintiff and Class members to provide their PII.

86. At all relevant times, Defendant CashCrate had a duty, or assumed a duty, to implement reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures and adequate third-party vendor and vendor software vetting and monitoring, in order to safeguard the PII of the Plaintiff and the Class members and to prevent the unauthorized access to and disclosures of the same.

87. A duty was also created due to the special relationship between Defendant CashCrate, as the entity with all knowledge and control regarding relevant and material facts concerning the nature in which it stores, maintains, and secures PII, and Plaintiff, as a customer who was required to provide her PII in order to use Defendant CashCrate's marketed services.

88. Defendant CashCrate breached the aforementioned duties in, including but not limited to, one or more of the following ways:

a. Failing to implement reasonable data privacy and cybersecurity measures to secure its or Plaintiff's and Class members' email accounts, including failing to require adequate multifactor authentication and encryption;

b. Failing to implement a reasonable data privacy and cybersecurity protocol, including adequate procedures for preventing cybersecurity threats and/or detecting such threats in a timely manner and adequate procedures for evaluating, vetting, monitoring, and selecting third-party vendors and third-party vendor software;

c. Failing to implement a reasonable patch management program;

d. Failing to notify Plaintiff and Class members that their PII had been disclosed within a reasonable period of time and/or through a reasonable manner or method;

e. Failing to reasonably comply with applicable state and federal law concerning its data privacy and cybersecurity protocol, including the substance and manner of any notification to Plaintiff and Class members concerning the Data Breach; and

f. Otherwise failing to act reasonably under the circumstances and being negligent with regards to its conduct in preventing, detecting, and disclosing the subject Data Breach.

89. Defendant CashCrate knew, or should have known, that its data privacy and cybersecurity protocol failed to reasonably protect Plaintiff's and the Class members' PII.

90. As a direct result of Defendant CashCrate's aforesaid negligent acts and omissions, Plaintiff and the Class members suffered injury and damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, and other pecuniary and non-pecuniary injury, including time and expense to mitigate the disclosure and/or significantly increased risk of exposure of their PII to nefarious third parties.

91. Wherefore, Plaintiff prays for the relief set forth below.

## COUNT VII
## Negligence
## (On behalf of Plaintiff and the Class and Subclass Against Defendant vBulletin)

92. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

93. Defendant vBulletin knew that the customers and users of its Forum Software licensees would need to provide their PII as a condition precedent to using the Forum Software.

94. Further, Defendant vBulletin knew of the risks associated with SQL-injection attacks, particularly with SQL-based software such as the Forum Software.

95. By offering its Forum Software for widespread commercial use and knowing that the security of the PII of millions of individuals was contingent on the integrity of the SQL-based Forum Software, Defendant vBulletin had a duty to implement reasonable data privacy and cybersecurity protocols, including adequate SQL monitoring and patch management procedures.

96. A duty was also created due to the explicit undertaking by Defendant vBulletin to provide "secure" forum software solutions, including the subject Forum Software, and its explicit undertaking to provide "world-renowned" ongoing technical support concerning the Forum Software, which should have included reasonable patch management and notification procedures.

97. Defendant vBulletin breached the aforementioned duties in, including but not limited to, one or more of the following ways:

a. Failing to implement reasonable cybersecurity practices that included adequate SQL monitoring and patch management;

b. Failing to reasonably notify affected Forum Software licensees of the Software Vulnerability;

c. Failing to take reasonable measures to ensure the Forum Software in use by its licensees was updated and not susceptible to SQL-injection attacks; and

d. Otherwise failing to act reasonably under the circumstances and being negligent with regards to its conduct in preventing, detecting, and disclosing the subject Software Vulnerability.

98. Defendant vBulletin knew, or should have known, that its SQL monitoring and patch management was inadequate to protect the PII of its Forum Software licensees' customers.

99. As a direct result of Defendant vBulletin's aforesaid negligent acts and omissions, Plaintiff and the Class members suffered injury and damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, and other pecuniary and non-

pecuniary injury, including time and expense to mitigate the disclosure and/or significantly increased risk of exposure of their PII to nefarious third parties.

100. Wherefore, Plaintiff prays for the relief set forth below.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class and Subclass set forth above, respectfully requests the Court order relief and enter judgement against Defendants:

A. Certifying the Class and Subclass identified above and appointing Plaintiff as Class representative and the undersigned counsel as Class counsel;

B. Awarding Plaintiff and the Class and Subclass appropriate relief, including actual, statutory, compensatory, and/or punitive damages;

C. Requiring Defendants to furnish identity fraud monitoring and mitigation services for a reasonable period;

D. Granting injunctive relief requiring Defendants to implement commercially reasonable security measures to properly guard against any and all future cyberattacks and to provide reasonable notification in the event of such an attack;

E. Requiring Defendants to pay Plaintiff's and the Class members' reasonable attorneys' fees, expenses, and costs; and

F. Any such further relief as this Court deems reasonable and just.

## DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

Dated: February 20, 2019

Respectfully submitted:

SHANICE KLOSS, individually and on behalf of a class of similarly situated individuals

By: /s/ Jad Sheikali
*One of Plaintiff's Attorneys*

Jad Sheikali
William Kingston
MCGUIRE LAW, P.C.
55 W. Wacker Dr., 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
jsheikali@mcgpc.com
wkingston@mcgpc.com

*Attorneys for Plaintiff and the Putative Classes*